Patent Claims

1. A method of transmitting signal/data sequences between a transmitter and a receiver with authentication of the transmitted signal/data sequences by using keys and cryptographic algorithms, which are implemented on the transmitter end as well as on the receiver end, characterized in that
in a preliminary calculation phase, data is calculated as a function of a secret key using cryptographic algorithms, and then in a subsequent transmission phase, authentication tokens for the signals are calculated from this data, authenticating both the signals as well as the sequence in which the signals are transmitted.

2. The method according to Patent Claim 1, characterized in that
in a preparatory phase, a pseudo-random sequence (PRS) is generated using a cryptographic algorithm;
certain strings of this sequence are used as a code for the signals of the signal supply as well as the transmitting stations (1, 2, ... MAX); and
the authentication token of the signal transmitted at the i-th (i = 1, 2, ..., MAX) position is calculated as a function of the coding of the signal and the coding of the transmission position (i).

3. The method according to Patent Claim 2, characterized in that
the authentication token (T) of the signal transmitted at the i-th position (i = 1, 2, ..., MAX) is the bit-by-bit XOR link or an equivalent logic function of the coding of the respective signal and the coding of the transmission position (i).

4. The method according to Patent Claim 1, characterized in that
a pseudo-random sequence (PRS) is generated in the preliminary calculation phase using a cryptographic algorithm;
certain strings of this sequence are used as the coding of the signals of the

signal supply as well as the transmitting stations (1, 2, ..., MAX); and the authentication token of the signal transmitted at the i-th position (i = 1, 2, ..., MAX) is calculated as a function of the coding of all the previously transmitted signals (1, 2, ..., i) and of the coding of the transmission position (i).

5. The method according to one of Patent Claims 1 through 4, characterized in that
the authentication token (T) of the signal transmitted at the i-th position (i = 1, 2, ... MAX) is the bit-by-bit XOR link or an equivalent logic link of the coding of all previously transmitted signals (1, 2, ... i) and the coding of the transmission position (i).

6. The method according to one of Patent Claims 1 through 5, characterized in that
the cryptographic algorithm used in the preliminary calculation phase is a block cipher.

7. The method according to Patent Claim 6, characterized in that
the known data encryption standard is used as the block cipher.

8. The method according to one of Patent Claims 6 or 7, characterized in that
the pseudo-random sequence (PRS) is generated by operating the block cipher in the known output feedback mode.

9. The method according to the definition of the species of Patent Claim 1 or according to one of Patent Claims 2 through 8, characterized in that
a token (T) for authentication of the respective transmitter is also calculated in the preparatory phase and is transmitted subsequently, initializing the receiver for authentication of the transmitter.

10. The method according to one of Patent Claims 1 through 9, characterized in that

the sequence of the transmitted signals is confirmed by nonintersecting m-bit strings (t(i)).

Add a'

Add B'